SEGURIDAD INFORMÁTICA Y EL MALWARE

García Monje, Robert Alexander
robertgmonje@hotmail.com
Universidad Piloto de Colombia

Resumen: *la seguridad informática busca mitigar los riegos (amenazas y vulnerabilidades) a los que están expuestos los sistemas informáticos; actualmente el riesgo más frecuente está relacionado con el malware, el cual es un programa informático desarrollado por ciberdelincuentes para beneficio propio, que tiene como objetivo sustraer información, afectar o dañar los sistemas informáticos.*

Abstract: *computer security seeks to mitigate the risks (threats and vulnerabilities) to which computer systems are exposed; currently the most frequent risk is related with the malware which is a computer program developed by cybercriminals for their own benefit, which have with objective to subtract information, affect or damage a computer system.*

Palabras claves: *amenaza, antivirus, confiabilidad, cortafuegos, disponibilidad, gusano, información, informática, integridad, malware, ransomware, riesgo, troyano, virus, seguridad.*

I. INTRODUCCIÓN

El mundo de hoy se ha vuelto dependiente del uso de sistemas informáticos como computadores, teléfonos inteligentes, entre otros, este tipo de dispositivos y la información que en ellos se almacena o es transmitida, se encuentra amenazada por intenciones malintencionadas de ciberdelincuentes que buscan copiar, sustraer o atentar contra su integridad.

Seguridad informática es un concepto que no todos tienen presente, puesto que se le relaciona solo con grandes infraestructuras tecnológicas y habilidades especializadas, cuando en realidad la seguridad informática aplica a cualquier sistema informático y usuario.

En general la seguridad informática se caracteriza por buscar:

- Confidencialidad: asegurar el acceso de la información, con autorización previa.
- Integridad: salvaguardar la precisión y exactitud de la información.
- Disponibilidad: asegurar que los usuarios autorizados, puedan acceder a la información cuando la necesitan.

Dado lo expuesto, resulta pertinente hablar sobre la seguridad informática y de manera particular abordar el tema de malware en este paper, en el desarrollo encontrará una descripción de que es el malware, sus principales tipos, métodos de propagación, síntomas de una posible infección, recomendaciones de prevención y una recopilación de los malware más peligros de la historia.

II. SEGURIDAD INFORMÁTICA

La informática o también llamada computación, hace referencia al almacenamiento, tratamiento automatizado y trasmisión de información, a través de hardware, software y redes de datos; busca asegurar que los sistemas informáticos y sus recursos generen valor en los usuarios, que se utilicen de la manera adecuada según las características y restricciones de cada clase de sistema informático, que el acceso a la información que en ellos se alberga sea adecuado para los fines establecidos, que su modificación solo sea posible para las personas que se encuentren autorizadas.

Los elementos principales que se deben proteger en cualquier sistema informático son: el hardware, el software, los datos e información; si bien es cierto que todos los elementos de un sistema informático están expuestos a un ataque de un ciberdelincuente, son los datos e información los elementos principales de protección y de la aplicación de medidas de seguridad.

El hardware comprende los elementos físicos (compuestos por elementos electrónicos, eléctricos, mecánicos entre otros) tales como computadores (y sus periféricos como impresoras, webcam, teclado,

etc.), tablets, smartphones, consolas de videojuegos, televisores entre otros, y sobre ellos gobiernan los software, los cuales son programas y aplicaciones (incluido los sistemas operativos) que hacen funcionar el hardware o realizar tareas determinadas a través de secuencias de instrucciones.

Las redes de datos corresponden a la interconexión de sistemas informáticos (anteriormente solo computadores, hoy cualquier objeto cotidiano con conexión a internet), con el objetivo de intercambiar información en tiempo real (comercio electrónico, correo electrónico, almacenamiento en la red, redes sociales, mensajería instantánea, gestión, entre otros), actualmente, internet es la mayor red de datos y cuenta con cobertura global. La unión e interacción del hardware, software y redes de datos se denomina sistema informático.

Teniendo en cuenta las anteriores descripciones, se puede decir que la seguridad informática se define como la búsqueda de mitigar los riesgos, en los que se ven inmersos todos los sistemas informáticos, estos riesgos son amenazas y vulnerabilidades para la integridad del hardware (daños) y/o la pérdida de la confidencialidad, integridad y disponibilidad de la información.

La seguridad informática se ocupa de generar buenas prácticas, destinadas a garantizar sistemas de información seguros y confiables antes posibles riesgos. La seguridad informática busca reducir la posibilidad de que se materialicen los riesgos.

Entre las amenazas que puede afectar los sistemas informáticos, se encuentran las acciones de ciberdelincuentes, que a través de ingeniería social y malware (o software malintencionado que más adelante se describe) buscan causar daño o perjuicio en el sistema informático de los usuarios como el robo de información, modificaciones al sistema operativo o a las aplicaciones instaladas, o tomar el control del equipo infectado. Es tarea de la seguridad informática y de cada usuario prevenir y tomar acciones de protección.

De acuerdo con una estadística sobre amenazas detectadas en sistemas informáticos, realizada por la compañía especializada en malware Kaspersky [1]:

- El 31,9% de las computadoras de los usuarios fueron sometidas al menos a un ataque de la clase malware durante el año.

  Entre estos malware se encuentran:

Tabla 1. Top amenazas detectadas (malware) más frecuentemente detectado en las computadoras de los usuarios en 2016. *[1]*

No.	Name	% of unique attacked users
1	DangerousObject.Multi.Generic	42.32
2	Trojan.Win32.Generic	9.23
3	Trojan.WinLNK.Agent.gen	7.78
4	Trojan.WinLNK.StartPage.gena	6.25
5	Trojan.Script.Generic	5.86
6	Trojan.Win32.AutoRun.gen	4.78
7	Virus.Win32.Sality.gen	4.34
8	Trojan.WinLNK.Runner.jo	4.17
9	Worm.VBS.Dinihou.r	3.58
10	Trojan.WinLNK.Agent.ew	3.13
11	Trojan.Win32.Starter.yy	2.93
12	Trojan-Downloader.Script.Generic	2.80
13	Trojan.Win32.Autoit.cfo	2.27
14	Trojan.Win32.Wauchos.a	2.03
15	Virus.Win32.Nimnul.a	2.02
16	Trojan-Proxy.Win32.Bunitu.avz	1.90
17	Worm.Win32.Debris.a	1.83
18	Trojan.Win32.Hosts2.gen	1.80
19	Trojan-Dropper.VBS.Agent.bp	1.34
20	Trojan.WinLNK.StartPage.ab	1.26

- Las soluciones de Kaspersky Lab repelieron 758.044.650 ataques lanzados desde recursos en línea ubicados en todo el mundo.

  Donde los países con más ataque fueron:

Tabla 2. Países Top donde los usuarios enfrentan mayor riesgo de infección. *[1]*

No.	Country	% of unique users
1	Russia	42.15
2	Kazakhstan	41.22
3	Italy	39.92
4	Ukraine	39.00
5	Brazil	38.83
6	Azerbaijan	38.81
7	Spain	38.21
8	Belarus	38.04
9	Algeria	37.11
10	Vietnam	36.77
11	China	36.53
12	Portugal	35.86
13	France	34.74
14	Armenia	33.01
15	Greece	32.99
16	Chile	32.82
17	India	32.61

No.	Country	% of unique users
18	Qatar	32.53
19	Indonesia	32.30
20	Moldova	31.42

- 261.774.932 URL fueron reconocidas como maliciosas por los componentes antivirus web.

- El 29,1% de los ataques web neutralizados por los productos Kaspersky, se realizaron utilizando recursos web maliciosos ubicados en los Estados Unidos.

- El antivirus web de Kaspersky, detectó 69.277.289 objetos maliciosos.

- 1.445.434 computadoras de usuarios fueron atacadas por cifradores.

- El antivirus de Kaspersky detectó un total de 4.071.588 programas maliciosos y potencialmente no deseados.

A. Malware

Malware o *malicious software* (software malicioso), hace referencia a cualquier programa o aplicación informática, que luego de infectar un sistema informático víctima, tiene como objetivo dañar de diferentes maneras a los sistemas informáticos (el malware puede afectar a los diferentes sistemas informáticos de acuerdo con el tipo de malware) de forma intencional y sin el consentimiento del usuario.

De acuerdo con su comportamiento, el malware puede clasificarse como gusanos, spyware, troyanos, ransomware y otros que se describen más adelante; por lo anterior se podría decir que malware se refiere a cualquier tipo de código malicioso o amenaza informática de tipo lógico, aunque se le llame solo virus.

1) Principales clases de malware

- *Virus*: son aplicaciones o programas elaborados con el fin de generar un mal funcionamiento del sistema operativo, atacan los archivos del sistema (generalmente los archivos ejecutables de las aplicaciones), modificándolos o borrandolos; para su activación y propagación requieren la ejecución de la aplicación infectada.

- *Gusanos*: son aplicaciones o programas que se implantan en los archivos propios del sistema operativo, con el objetivo de ejecutarse y propagarse, sin necesidad de la intervención del usuario.

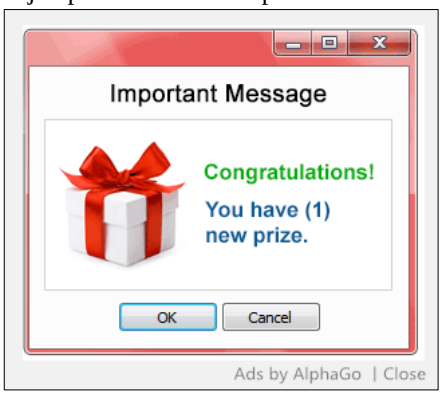
- *Spyware*: son aplicaciones o programas que se instauran en el sistema, generalmente con el propósito de recopilar información del usuario almacenada en el sistema informático sin su autorización; ésta información es enviada al desarrollador del spyware generalmente para usos publicitarios.

- *Troyanos*: son aplicaciones o programas que tienen como objetivo permitir de forma oculta y remota la instalación de gusanos o spyware; comúnmente estos se alojan en programas o aplicaciones, simuladamente legítimas, por lo cual al ejecutarse actúan de forma silenciosa.

- *Phishing*: tiene como objetivo recolectar información de autenticación de sitios web del usuario (información de bancos, cuentas de correo, redes sociales, entre otros); a través de un archivo ejecutable o un enlace enviado vía correo electrónico, el usuario es direccionado a un sitio web falso, diseñado para que el usuario sienta que ingresa al sitio web legitimo e ingrese su información confidencial de acceso (usuario, contraseña, entre otros).

- *Adware*: son aplicaciones desarrolladas en torno a la publicidad, pueden generar automáticamente ventanas con publicidad, direccionar al usuario a sitios web de publicidad, y en algunos casos, también recopilan información sobre los hábitos del usuario (horas del día en que se conecta, sitios que visita, etc.).

Figura 1. Ejemplo de ventana de publicidad adware. *[2]*



- *Rootkits*: son programas desarrollados para permitirle a terceros (normalmente el desarrollador) tener acceso no autorizado a un sistema informático, trabajan de forma silenciosa por lo que es muy difícil que el usuario o un software antivirus los detecten.

- *Keylogger*: software desarrollado para capturar todo lo que el usuario escribe en el teclado del sistema informático (el objetivo principal es obtener nombres de usuario, contraseñas, etc.), e incluso algunos más avanzados registran las actividades del mouse y cualquier otro elemento de entrada; la información recolectada es trasmitida a terceros, normalmente, el desarrollador del keylogger.

- *Ransomware*: es una aplicación que retiene o secuestra la información del usuario (a través de algoritmos de cifrado de datos) o realiza restricciones al sistema, (inhabilitando el sistema informático) para luego solicitar al usuario un pago económico (rescate de la información o habilitar el sistema informático).

Figura 2. Ejemplo de notificación de secuestro de datos (ransomware). [3]

- *Backdoors*: son programas informáticos, que tienen como objetivo, abrir una puerta trasera en el sistema informático donde se aloja, permitiendo a un tercero (generalmente el desarrollador) tener acceso y control del sistema.

- *Botnet*: denominación para un grupo de sistemas informáticos infectados por un código malicioso, que permite al atacante controlar el equipo para realizar determinadas tareas (motivo por el cual también se les denomina zombis), como el envío masivo de spam o masivos ataques de denegación de servicio (DDoS).

- *Rouge*: son programas informáticos (o sitios web) que no son lo que dicen ser, estos generalmente se anuncian como software de seguridad gratuitos (antivirus que garantizan eliminar falsas infecciones detectadas) y al ser ejecutados por el usuario, instalan otro tipo de malware en el sistema informático infectado.

Figura 3. Ejemplo malware Rouge "System care antivirus". [4]

2) *Métodos de distribución o contagio*

El principal motivo de infección de los sistemas informáticos es causado por el usuario, quien ejecuta el virus y permite la instalación sin saberlo; en segundo lugar, están los gusanos que infectan el sistema informático donde se encuentra y se replican a través de la red.

A continuación, se definen los principales medios y técnicas para distribuir e intentar infectar los sistemas informáticos:

- *Ingeniería social: l*a técnica de la ingeniería social es un gran reto que afronta la seguridad informática, ya que actúa directamente sobre la víctima manipulándola psicológicamente mediante el engaño, para que comparta información confidencial (credenciales de acceso, nombres de usuario, contraseñas, etc.) o realice acciones inseguras (ejecución de algún archivo o deshabilitación de alguna función).

  Los ataques de ingeniería social más comunes se realizan a través de correos electrónicos de phishing, donde se envían múltiples correos electrónicos engañosos que solicitan algún tipo de información privada, requieren la apertura de algún archivo o llevan al usuario a un sitio web en particular. Otra técnica de ingeniería social ya no usada frecuentemente (debido a la capacidad que tiene los antivirus de detectar una amenaza antes de ser ejecutada), se realiza a través de memorias USB o CD/DVD cargadas de malware, que se le hace llegar a la víctima como aparentemente inofensivas, una vez son instaladas en el sistema informático el malware se instala.

- *Correo electrónico*: valiéndose de este popular medio de comunicación, hacen llegar a los usuarios el virus en forma de archivo adjunto de un correo, normalmente, estos mensajes suplantan la información del remitente con el objetivo de generar confianza y que los receptores ejecuten el virus.

- *Aplicaciones P2P*: también conocidas como aplicaciones punto a punto, las cuales generan una red virtual de sistemas informáticos, en la que cada computadora actúa como un nodo servidor/cliente al mismo tiempo, con el objetivo de intercambiar información de forma directa; normalmente se usa para compartir aplicaciones, vídeos, música, películas y es ahí donde nace el riesgo de ser infectado, ya que estas descargas pueden estar infectadas por códigos maliciosos. Entre las aplicaciones más populares de P2P se pueden encontrar a Emule, Ares, Utorrent y FilesWire.

- *Sitios Web*: a través de páginas web fraudulentas o infectadas, estas emiten mensajes al usuario solicitando que instale complementos para poder ver el contenido (códigos maliciosos) o presentan ventanas emergentes donde se anuncian premios y deben hacer clic para continuar instalando el virus.
- *Memorias USB, CD, DVD*: dada su popularidad y su facilidad para portar y compartir información, son un buen método para propagar malware; para ello, los códigos maliciosos crean un archivo llamado autorun.ini, el cual contiene instrucciones para que Windows ejecute automáticamente el ejecutable del virus.

- *Agujeros de seguridad:* se aprovechan de las fallas de seguridad no detectadas por desarrollares en los sistemas operativo de los navegadores web y aplicaciones en general; estos fallos son detectados por los virus para infectar los sistemas informáticos.

3) Síntomas de infección por malware

Dado el grado de complejidad en la elaboración del malware (cada día surgen nuevas amenazas con objetivos y comportamientos diferentes, capaces de ser casi indetectables) es difícil identificar si un sistema informático está infectado a simple vista, pero existen algunas señales que pueden alertar al respecto. En todo caso, siempre es recomendable el uso de un software antivirus para identificar si realmente el sistema se encuentra infectado por malware ante cualquier comportamiento anormal.

A continuación, se relacionan algunos de los principales síntomas que pueden estar relacionados con una infección:

- *Ventanas emergentes*: frecuentes ventanas emergentes en el escritorio (pop-up) o en el navegador web con mensajes que se abren sin que el usuario tome acción al respecto son síntoma de infección por malware; estas ventanas suelen contener información de publicidad, solicitudes de instalación de software, solicitudes de actualizaciones del sistema operativo o de un programa en particular, reportes de falsas infecciones de malware que debe ser eliminados.

Figura 4. Síntoma de infección: ventana emergente. [5]

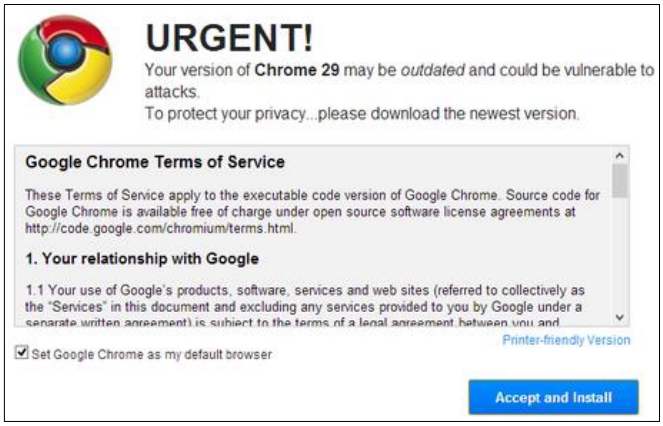
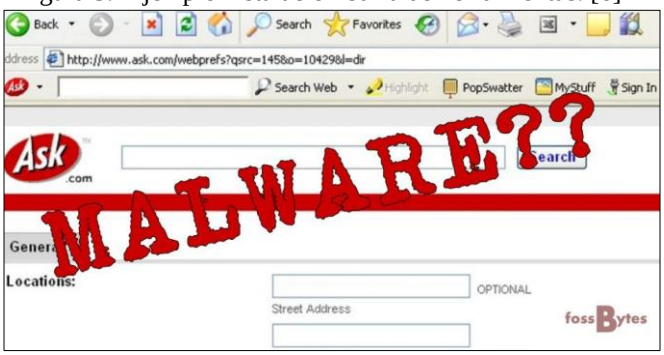


Figura 5. Ejemplo instalación barra de herramientas. [6]



- *Lentitud del sistema*: es un síntoma realmente relativo, ya que la lentitud en un sistema informático puede ser causado por múltiples causas, entre estas la posibilidad de que un malware está consumiendo los recursos del sistema (procesador, memoria, almacenamiento) causando que la respuesta del sistema y de los programas tarde más de lo habitual.

- *Mal funcionamiento del sistema*: algunos malware afectan archivos esenciales del sistema, toman control de funcionalidades del sistema operativo o de los navegadores web causando errores y comportamientos anómalos como mostrar ventanas de errores, desbordamientos de memoria y problemas de compatibilidad de hardware (pantalla azul), lentitud o congelamiento de aplicaciones, falta de respuesta de los periféricos (mouse, impresora y teclado, etc.), problemas para abrir aplicaciones o cierres inesperados de aplicaciones, borrado de accesos directos a programas o archivos, etc.

- *Barras de herramientas*: algunos malware disfrazados de programas gratuitos instalan barras de herramientas (o de búsquedas) en los navegadores web; también es común que realicen cambios en la página de inicio y buscador por defecto, generando que las búsquedas realizadas en el equipo infectado sean redirigidas a otro sitio web que no necesariamente es un buscador.

- *Desafiliación del antivirus o firewall*: algunos malwares actúan directamente sobre los antivirus o firewall deshabilitándolos silenciosamente sin intervención de usuario y dejando vulnerable el sistema informático para la instalación de nuevos malware.

- *Archivo y carpetas*: comportamientos extraños en la estructura de archivos y carpetas (falta de archivos o carpetas, renombrado, cambio de extensión, no se puede abrir) puede ser un síntoma de infección por malwares, algunos están diseñados para borrar o cifrar información.

- *Cambio de idioma de aplicaciones o sistema operativo*: aplicaciones que se presentan en un idioma diferente al instalado puede ser un síntoma de infección, algunos malware para ejecutarse correctamente en el sistema infectado requieren modificar el idioma del sistema operativo o de la aplicación en la que se alojan.

- *Comportamiento conexión a internet*: si al conectarse se presentan múltiples ventanas del navegador con páginas no solicitadas (algún malware tiene como fin redirigir la navegación) o si a pesar de que no se está realizando descargas, el servicio de internet es muy lento (el malware puede estar realizando tareas que consumen ancho de banda), puede que el sistema informático está infectado por malware.

- *Inusual actividad del disco duro*: si el sistema al estar en estado de quietud (sin realizar tareas determinadas por el usuario) se observa alta

actividad del disco duro, puede ser un signo de que el sistema informático está infectado por un malware que está realizando tareas con los archivos.

4) *Métodos de prevención*

Mencionados los que podrían considerarse los más importantes malware que pueden afectar a los sistemas informáticos y principales métodos de distribución o contagio, a continuación se relacionan algunas buenas prácticas de prevención:

- *Antivirus*: son aplicaciones o programas informáticos diseñados para detectar y eliminar virus. Se recomienda instalar uno en los sistemas informáticos y éste debe configurarse para que revise todo el sistema periódicamente; también es necesario verificar con frecuencia que está activo (los antivirus pueden desactivarse por error del usuario o por un virus). Debido a que día a día aparecen nuevos virus, actualice su antivirus (se actualiza la base de datos de virus) de forma que el antivirus pueda garantizar una protección ante nuevas amenazas.

  Ejemplos de antivirus:

  - Defender
  - Kaspersky
  - Bitdefender
  - Panda
  - AVG
  - Avast

  Antivirus online:

  - Virustotal
  - Virscan
  - Jotti's malware scan

- *Cortafuegos*: también llamados firewall es una aplicación o programa diseñado para garantizar la seguridad de las conexiones a internet, éste realiza monitoreo a las comunicaciones entrantes y salientes de un sistema informático y bloquea las entradas o salidas de información sin autorización; algunos desarrolladores incluyen la función de antivirus en las aplicaciones de firewall. Para los casos de los sistemas informáticos que cuentan con conexión permanente a internet a través de una dirección Ip pública fija, es recomendable instalar una aplicación de este tipo.

  Ejemplos de cortafuegos:

  - Defender Panda Internet Security
  - Comodo Firewall
  - ZoneAlarm Free
  - PrivateFirewall
  - Emsisoft Internet Security

- *Actualizaciones*: actualice frecuentemente el sistema operativo y las aplicaciones instaladas en el sistema informático con los parches de seguridad que distribuyen las compañías desarrolladoras de las aplicaciones; normalmente, estas actualizaciones se realizan de manera automática previa autorización del usuario y tienen como fin especial reducir las vulnerabilidades que se encuentran en las aplicaciones más populares como los navegadores de internet, procesadores de texto, programas de correo, etc.

- *Software legal*: las aplicaciones piratas suelen contener virus, spyware u otros tipos de códigos maliciosos, por lo cual es recomendable instalar en los sistemas informáticos solamente aplicaciones legales y que provengan de fabricantes conocidos.

- *Correo electrónico*: antes de abrir los correos electrónicos recibidos, desconfíe de los mensajes de remitentes desconocidos con adjuntos o vínculos dudosos, como también desconfié de mensajes con contenidos que no esperaba y enviados desde un remitente conocido; en caso de no poder verificar la confiabilidad de estos mensajes elimínelos.

- *Archivos*: no abrir aplicaciones, archivos, documentos, etc., que no esté completamente seguro de que son y que provienen de una fuente confiable; someta a revisión de la aplicación antivirus cada nuevo archivo. No descargue archivos de fuentes desconocidas de internet ni de redes P2P.

- *Sitios web*: desconfíe de las páginas web desconocidas y aquellas dónde podrá encontrar

software gratuito o promociones de artículos con precios bajos o premios.

Tabla 3. Windows anti-malware market share reports. *[7]*

No.	Name	% Market share
1	AVAST Software a.s.	20.55%
2	ESET	13.36%
3	McAfee, Inc.	9.48%
4	Avira GmbH	7.73%
5	Safer-Networking Ltd.	7.46%
6	Malwarebytes Corporation	6.88%
7	Qihu 360 Software Co., Ltd.	5.14%
8	Kaspersky Lab	5.12%
9	Webroot Inc	4.96%
10	Bitdefender	4.2%

5) *Malware más peligros de la historia*

Al realizar una búsqueda en fuentes abiertas sobre los principales malwares con más impactos en la historia, se encuentran los que presentan en la siguiente tabla:

Tabla 4. Malware más peligros de la historia. *[8]*

Año	**Malware**	**Tipo**
1998	CIH	Virus
1999	Melissa	Gusano
2000	Iloveyou	Gusano
2001	Code red	Gusano
2003	Slammer	Gusano
2003	SoBig.F	Gusano
2004	My doom	Gusano
2010	Stuxnet	Gusano
2013	Cryptolocker	Ransomware
2013	Zeroaccess	Botnet
2016	Locky	Ransomware
2017	Wannacry	Ransomware

- *CIH*: también llamado Chernobyl, realizaba un borrado de los datos de los discos duros y en algunos casos también borraba el firmware del chipset bios de los sistemas informáticos infectados.

- *Melissa*: este virus se alojaba y modificaba los documentos de Word de Microsoft office; sé auto propagaba a través de Microsoft Outlook enviando el virus los 50 primeros contactos de la libreta de direcciones.

- *Iloveyou*: trasmitido como archivo adjunto "Love letter for you" vía correo electrónico, al ser ejecutado, modifica la información del sistema informático víctima y se enviaba a todas las direcciones registradas en libreta de direcciones.

- *Code red*: pertenece a la categoría de gusanos el cual afectaba servidores web de Microsoft internet información server (Web IIS), podía ejecutarse directamente desde la memoria de procesos y realizaba ataques de denegación de servicio a importantes sitios web.

- *Slammer*: es un gusano de denegación de servicio DDoS que atacaba servidores SQL de Microsoft causando que se extendiera rápidamente por el mundo, produciendo lentitud en el tráfico de internet a nivel mundial.

- *SoBig.F*: se propaga con rapidez vía correo electrónico y carpetas compartidas; una vez infectado, abre una puerta trasera en el sistema informático y se intenta propagar enviándose a todas las direcciones registradas en libreta de direcciones.

- *My doom*: considerado uno de los malwares que más rápido se propagó en el mundo, principalmente como archivo adjunto vía correo electrónico, al ser ejecutado busca en archivos locales direcciones de correo electrónico para enviarse; adicionalmente se ubicaba en carpetas compartidas de servicios de intercambio de archivos P2P.

- *Zeus*: gusano cuyo objetivo eran los sistemas de control industrial Scada, se trasmitía manualmente a través de memorias USB y una vez infectado, realizaba una comprobación si tenía acceso a sistemas Scada para permitir al atacante tener control.

- *Cryptolocker*: clasificado como ransomware, es trasmitido como archivo adjunto vía correo electrónico o a través de red; cifra los discos duros de las víctimas para luego pedir un pago de rescate en un tiempo límite.

- *Zeroaccess*: este tipo de malware atacaba sistemas informáticos y luego convertirlos en botnet para realizar diferentes actividades maliciosas como envió de correos spam, ataques de denegación de servicio

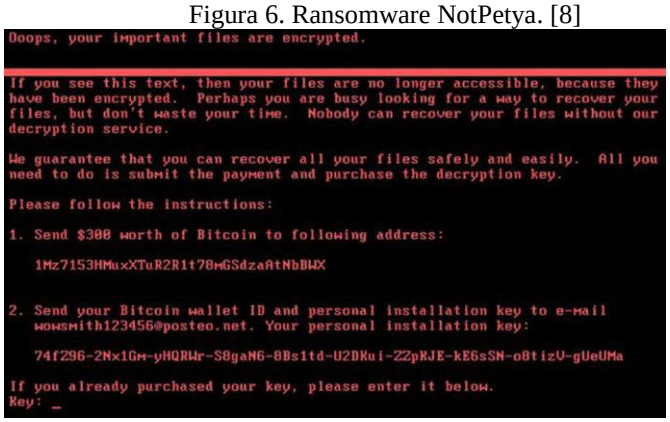
DDoS, minería de bitcoins, etc.

- *Locky*: se propaga a través de macros de Microsoft word, éste bloquea los archivos del disco duro de la víctima y cualquier unidad de red con cifrado (además renombra las extensiones por "Locky") para luego solicitar un pago para desbloquearlos.

- *Wannacry*: este ransomware aprovechaba una vulnerabilidad del sistema operativo Windows para propagarse vía red; al infectar la víctima, encripta los archivos del sistema informático para luego pedir un rescate.

- NotPetya: es un ransomware que además de cifrar la información del sistema informático infectado, también restringe el ingreso al sistema operativo una vez es reiniciado, para luego solicitar un rescate; de este modo, el usuario deberá pagar el rescate o reinstalar el sistema operativo del sistema informático.

Figura 6. Ransomware NotPetya. [8]



III. CONCLUSIONES

El crecimiento en el uso de sistemas informáticos nos exponen a ser vulnerables a diferentes tipos de malware, que en general pueden ser definidos como: cualquier tipo de código malicioso que puede afectar la integridad y confiabilidad de los sistemas informáticos; como también la información que en ellos se alojan y su privacidad; es por ello que la seguridad informática es de gran importancia, ya que permite comprender los riesgos y las herramientas para prevenir perdida o el robo de información.

Es importante comprender que la confidencialidad de la información debe ser una prioridad no solo para expertos en temas de seguridad informática, sino de cualquier usuario, quien debe ser consciente que el uso de sistemas informáticos trae consigo un riesgo para la información y la privacidad; una prevención inicial para reducir los riesgos es actuar con precaución y tomar medidas de seguridad.

Para mantener un sistema seguro se debe seguir buenas prácticas en seguridad informática como mantener el sistema operativo actualizado y los navegadores web, instalar un antivirus o cortafuegos y mantenerlo actualizado; actuar siempre con precaución no abriendo archivos de procedencia dudosa como los provenientes de correos electrónicos extraños, evitar realizar descargas de contenidos desde fuentes P2P o sitios web de software gratuitos.
La ingeniería social actúa directamente sobre la interacción humana (los usuarios son el eslabón más débil) sobre los sistemas informáticos, por lo cual medios técnicos o tecnológicos de prevención en seguridad informática no pueden prevenir los ataques, razón por lo tanto es importante que los usuarios de sistemas informáticos estén alertas y tengan buenos hábitos de seguridad, siendo prioridad para evitar los malwares.

IV. REFERENCIAS

[1] «Kaspersky Security Bulletin OVERALL STATISTICS FOR 2016,» Kaspersky , 2016. [En línea]. Available: https://kasperskycontenthub.com/securelist/files/2016/12/Kaspersky_Security_Bulletin_2016_Statistics_ENG.pdf. [Último acceso: 1 Julio 2017].

[2] «How to Remove AlphaGo Adware – Easy & Effective Guide – PC Malware Issues Fix,» [En línea]. Available: http://icleansoftware.com/how-to-remove-alphago-adware-easy-effective-guide/. [Último acceso: 10 Julio 2017].

[3] A. Ardións, «Qué es Ransomware,» [En línea]. Available: https://androidphoria.com/seguridad/que-es-Ransomware. [Último acceso: 10 Julio 2017].

[4] Softonic, «Advanced SystemCare with Antivirus,» [En línea]. Available: https://advanced-systemcare-with-antivirus.en.softonic.com/. [Último acceso: 10 Julio 2017].

[5] J. Acevedo, «Protégete ante falsos avisos de actualización,» [En línea]. Available: http://www.pcworldenespanol.com/2013/09/17/protegete-ante-falsas-actualizaciones-y-avisos-de-actualizacion/. [Último acceso: 10 Julio 2017].

[6] «Hardware y Software,» 26 Junio 2017. [En línea]. Available: https://computacioncpc.files.wordpress.com/2011/06/teorc3ada-hardware-y-software.pdf.

[7] O. Metadefender, «Windows Anti-malware Market Share Reports,» [En línea]. Available:

https://www.metadefender.com/reports/anti-malware-market-share#!/. [Último acceso: 10 Julio 2017].

[8] R. Garcia, *SEGURIDAD INFORMÁTICA Y EL MALWARE,* Bogota, 2017.

[9] T. Fox, «Petya Or NotPetya: Why The Latest Ransomware Is Deadlier Than WannaCry,» [En línea]. Available: https://www.forbes.com/sites/thomasbrewster/2017/06/27/petya-notpetya-ransomware-is-more-powerful-than-wannacry/#59fccce9532e. [Último acceso: 10 Julio 2017].

[10] M. Rivero, «10 posibles síntomas para saber si tu PC está infectado.,» [En línea]. Available: https://www.infospyware.com/articulos/10-posibles-sintomas-para-saber-si-tu-pc-esta-infectado/. [Último acceso: 2017 Julio 08].

[11] G. González, «Identifica los síntomas de un PC infectado con malware,» 08 07 2017. [En línea]. Available: http://blogthinkbig.com/aprende-identificar-los-sintomas-pc-infectado-malware/.

[12] J. Dunn, «12 of the world's most deadly ransomware,» 2017. [En línea]. [Último acceso: 20 Junio 2017].

[13] Axarnet, «Cómo reconocer si tu pc está infectado,» 2017. [En línea]. Available: https://www.axarnet.es/blog/como-reconocer-si-tu-pc-est%C3%A1-infectado/. [Último acceso: 3 07 2017].

[14] «Spam and phishing in Q1 2017 - Securelist,» 2017. [En línea]. Available: https://securelist.com/spam-and-phishing-in-q1-2017/78221/. [Último acceso: 24 Junio 2017].

[15] «Sintomas de infeccion de malware,» 10 07 2017. [En línea]. Available: http://www.forospyware.com/t266312.html.

[16] «Most Destructive Malware of All Time,» 2017. [En línea]. Available: https://www.opswat.com/blog/most-destructive-malware-all-time. [Último acceso: 23 Junio 2017].

[17] «Malware - Panda Security Mediacenter,» 2017. [En línea]. Available: http://www.pandasecurity.com/spain/mediacenter/malware/. [Último acceso: 28 Junio 2017].

[18] «Los tipos de malware,» 28 Junio 2017. [En línea]. Available: https://support.kaspersky.com/mx/614.

[19] «Los 5 Virus Informáticos Más Destructivos De Todos Los Tiempos,» 2017. [En línea]. Available: http://blog.hostdime.com.co/los-5-virus-informaticos-mas-destructivos-de-todos-los-tiempos/. [Último acceso: 20 Junio 2017].

[20] «Hackers han usado Ask Toolbar para inyectar malware,» 10 7 2017. [En línea]. Available: http://soluciones-inteligentes.co/articulo-hackers-han-usado-ask-toolbar-para-inyectar-malware.

[21] «El gusano Stuxnet | Symantec,» 2017. [En línea]. Available: https://www.symantec.com/es/mx/page.jsp?id=stuxnet. [Último acceso: 25 Junio 2017].

[22] «Cómo detectar malware,» 5 07 2017. [En línea]. Available: http://es.wikihow.com/detectar-malware.

[23] B. D. J, «Malware,» 25 06 2017. [En línea]. Available: http://www.bolanosdj.com.ar/TIC/MALWARE.PDF.

[24] «Definición de Seguridad Informática,» [En línea]. Available: https://protejete.wordpress.com/gdr_principal/definicion_si/. [Último acceso: 10 Junio 2017].

[25] «Actividad Virus y otras amenazas,» 25 Junio 2017. [En línea]. Available: http://aunclicdelmundo.obolog.es/actividad-virus-otras-amenazas-2228555.

[26] M. Rivero, «¿Qué son los Malwares?,» 27 Junio 2017. [En línea]. Available: https://www.infospyware.com/articulos/que-son-los-malwares/.

[27] «La Informática,» 30 Junio 2017. [En línea]. Available: https://www.informatica.us.es/index.php/conoce-tu-futura-escuela/la-informatica.

[28] «Seguridad Informatica UD01,» 28 Junio 2017. [En línea]. Available: http://es.scribd.com/doc/219971644/Seguridad-Informatica-UD01#scribd.

[29] «Utilizainternetsinmiedo.com,» 30 Junio 2017. [En línea]. Available: http://utilizainternetsinmiedo.com/blog/4-vias-infeccion-virus/.

[30] «Que es Hardware y Software,» 26 Junio 2017. [En línea]. Available: http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-Hardware-y-Software.php.

[31] «'NotPetya' Ransomware Locking Down Computers Across the World - ExtremeTech,» 'NotPetya' Ransomware Locking Down Computers Across the World - ExtremeTech, 2017. [En línea]. Available: https://www.extremetech.com/internet/251711-notpetya-ransomware-locking-computers-across-world. [Último acceso: 9 Julio 2017].

[32] «La ingeniería social: el ataque informático más peligroso,» ENTER.CO, 2016. [En línea]. Available: http://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/. [Último acceso: 5 Julio 2017].

[33] «5 cosas que debes saber sobre la Ingeniería Social,» WeLiveSecurity, 2016. [En línea]. Available: https://www.welivesecurity.com/la-es/2016/01/06/5-cosas-sobre-ingenieria-social/. [Último acceso: 5 Julio 2017].

AUTOR

Ingeniero electrónico, especialista en gerencia de proyectos con certificación PMI CAPM, estudios culminados de especialización en seguridad

informática; candidato a máster en gerencia de sistemas de información y proyectos tecnológicos; con más de 10 años de experiencia profesional, en áreas de proyectos tecnológicos, comunicaciones y logísticos; preventa de tecnología, desarrollo de requerimientos, seguimiento a clientes y soporte posventa.